APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/277,335	03/26/1999	DEAN A. KLEIN	MPATENT.053A	3400

20995   7590   11/04/2002

KNOBBE MARTENS OLSON & BEAR LLP
2040 MAIN STREET
FOURTEENTH FLOOR
IRVINE, CA   92614

EXAMINER
LEE, CHI-CHUNG E

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 11/04/2002

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 07-01)

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on *10 September 2002* .

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-14* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-14* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

    If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

        1.☐ Certified copies of the priority documents have been received.

        2.☐ Certified copies of the priority documents have been received in Application No. _____ .

        3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

    a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)	4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)	5) ☐ Notice of Informal Patent Application (PTO-152)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .	6) ☐ Other: .

DETAILED ACTION

Claim Rejections - 35 USC § 103

1.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or
> described as set forth in section 102 of this title, if the differences between the subject
> matter sought to be patented and the prior art are such that the subject matter as a whole
> would have been obvious at the time the invention was made to a person having ordinary
> skill in the art to which said subject matter pertains. Patentability shall not be negatived
> by the manner in which the invention was made.

2.   Claim1 – 4, 7-12 **remain rejected** under 35 U.S.C. 103(a) as being unpatentable over

Pond (US 4,864,616) in view of **Computer Dictionary.**

Claim 1 is directed to a method of storing data in a magnetic or optical storage media.

The method is practiced in a computer comprises steps of retrieving, generating, and encryption.

Pond is directed to a method of storing data in a protected form for retrieval by authorized

parties. The method includes use of plurality of IDs, 12, including master ID, machine ID,

configuration ID, primary ID, and secondary ID. These IDs are used to generate various keys,

14, which are input to a key stream generator is for generating key streams 16, 20, 22, 24, and 26

(see Col. 5 lines 44-59; Col. 3 lines 19-23). These key streams are used to encrypt plain text and

decrypt encoded text (see Col. 5 lines 60-61). Column 6 lines 35-54 disclose that data encrypted

with the key streams becomes a protected file. The examiner asserts that this disclosure clearly

suggests use of storage means for storing the protected file.

Pond differs from the claimed invention in that it fails to disclose use of magnetic or

optical storage for encrypted data and use of **non-erasable memory** for storing the ID code.

As disclosed in Computer Dictionary, use of **non-erasable memory, such as ROM**, was

known prior to applicant's filing date. Motivation to use **non-erasable memory, such as ROM**,

to store the master ID, machine ID, configuration ID, primary ID, and secondary ID would have

been the ability to prevent loss of IDs during power failure. In addition, the computer Dictionary

discloses use of a magnets-optical disc was known prior to applicant's filing date. Motivation to

use a magnets-optical disc to store the protected data would have been the ability to update the

data.

3.   As per claim 2, Pond is directed to retrieve the ID key stream (i.e. information)

corresponding to each of the identifiers from the label (i.e. memory) for decrypting the file (see

col. 9 lines 64-67; col. 3 19-62). Claim 2 is directed to retrieve information from memory,

decrypt the data response to the information and store it to one of the data storage.

4.   As per claim 3, Pond is directed to a method of defining the relationship between the IDs,

keys, and key streams. For each ID, a corresponding random-like number, called key, is

generated and utilized to seed a key stream generator to generate a key stream (see col. 5 lines

44-59; Figure 1).

5.   As per claim 4. Pond is directed the method of using ciphering processor to decrypt the

file label that comprise a key mix. The checksum process is then used to verify that the key mix

of the label has not been tampered with (col. 4 line 21 – 36; Figure 4). Finally, the examiner

averts that use of distributed processing in computer related arts is well known. As discuss in

Computer Dictionary, use of distributed processing was known prior to applicant's file date.

Motivation to use a distributed processing is to share workload in the computer system.

Claim 3 –4 are rejected.

6.   Claim 7 is rejected on the same bases as claim 1

7.   As per claim 8, Pond discloses use of a machine Id as part of the key to generate a key

stream, see Figure 1. Claim 8 is rejected.

8.   As per claim 9, the examiner asserts that if multiple bits were needed to store the number,

then it would be obvious to make use of the necessary number of bits. Claim 9 is rejected.

9.   As per claim 10, see figure 1. Claim 10 is rejected.

10.   As per claim 11, use of nonvolatile memory was address in the rejection of claim 1.

Claim 11 is rejected.

11.   As per claim 12, see col. 5 lines 1- 45. Claim 12 is rejected.

12.   Claim 5 – 6 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Pond** in view

of **Computer Dictionary** as applied claim1 above and further in view of **Nishino**.

13.   Nichino is directed to a method of using a secret number (i.e. hardware ID) stored on a

memory card of an IC card (i.e. memory integrated circuit). This ID is employed as a key and is

used for the encoding.   Thus use of IC card (non-volatile memory integration circuit) to store

key related data is well known. The examiner asserts that it would have been obvious to store

the ID's used to generates the key stream data would have been to keep this data in a secure and

readily available location. Claim 5 is rejected.

14.   As per claim 6 use of a serial data bus is well known and the examiner takes official

notice of such motivation to use a serial data bus to connect the card reader to the encryption

modules of the Pond-Nichono combination would have been to provide a reliable effective method of transmit input data the site of processing. Claim 6 is rejected

15.   **As per added claim 13**, Pond is directed to the data ciphering processor (i.e. encrypting device) to encrypt clear text and to decrypt encoded text (see. Column 5 lines 60-61). The file is automatically decrypted when read from (i.e. data storage medium) and encrypted when written to (i.e. data storage medium) in the manner that is transparent to the user (see column 5 lines 4-9). The examiner asserts that the data ciphering processor is connected and controlled (i.e. positioned in a data path) by CPU to receive the instructions for encrypting and decrypting sensitive data. Claim 13 is rejected.

16.   **As per claim 14**, Pond is directed to utilize a file label that is prefixed to the file. The label includes a Key Mix field which is a single byte containing five bit flags. One of the bits is a Label-is-Present flag that indicates whether the label is to be considered on the protected file. The Label-is-Present flag can be disabled as if the file were not encrypted (see column 6 lines 6-34). The examiner asserts that the Label-is-Present flag can be enabled to make sure all the protected files (i.e. all data) has been encrypted before transmitting to the data storage. Claim 14 is rejected.

Response to Argument

17.   Applicant **argues that** there is no teaching or suggestion in Pond that the memory for storing the machine ID is *non-erasable*. **In Response:** Pond specifically discloses that a Machine ID (MID) comprising a data string uniquely identifying each personal computer (see column 5 lines 22-24) is used to generate a corresponding MID key and MID key stream to encrypt the text (see column 5 line67 – column 6 line 2). The MID is utilized to generate 8-bytes

random-like binary keys which may be stored in the secure memory (see column 3 lines 19-21).

Once the MID is selected to encrypt the file, the file can be decrypted only on the computer on

which it was encrypted (see column 6 lines 45-47). The MID key is generated by MID is a bit

pattern which is used in the encryption process and which may be stored in a secure portion of

the PC's memory (see column 5 lines 35-40).

Thus it would have been clear to one of ordinary skill in the art that the MID plays

important role in copy protection system of personal computer.

The examiner asserts that allowing a user to change the MID would have allowed one of

ordinary skill in the art to allow a different computer to decrypt the secure data in Pond s since

the MID is selected to encrypt the file and the file can be decrypted only on the computer on

which if was encrypted. This it is clear one of ordinary skill in art would not wish to allow the

MID to be changed or the copy protection system of Pond would be compromised.

One well-known way of preventing changes to stored data would be using a ROM

because it's a semiconductor-based memory that contains instructions or data that can be read

but not modified. ROM and PROM are existing *non-volatile/ non-erasable* memory.

The motivation to keep the MID in a ROM memory (i.e. non-erasable memory) like MID

key is to assure no user can modify it once it was assigned. It prevents the user from changing

the MID of the existing computer to different MID of other computer so that the encrypted files

protected by the existing MID can be copied to other computer and decrypted by different MID.

Encryption of data also provides a high level of protection even if data storage medium is

physically stolen (see column 5 lines 1-3) because the MID cannot be figured out. The

Computer dictionary discloses the ROM, acronym for read-only memory, serving as a memory

that contains instructions or data that can be read but not modified whether paced there by

manufacturing or by a programming process. The examiner asserts that ROM is the secure

memory in the computer to contain important data or instructions.

18.   The applicant states that the identification code is stored in a *non-erasable* memory; such

as ROM or EPROM. The examiner disagrees. The EPROM is not *non-erasable* memory.

Response to Amendment

19.   The claim 8 of applicant's amendment (paper number 8) filed on 9/10/02 and supplement

amendment filed on 10/9/02 have not been entered because the applicant has filed a markup

version of amended claim 8 without submitting a clear one.

20.   Applicant added claims 13, 14 has been addressed above.

21.   Claims 1,5,7,8 have been amended.

22.   Applicant has amended claim 8 to overcome the rejection of 35 USC 112.

23.   Examiner withdraws the objection to the specification.

Conclusion

24.   **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time

policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within TWO

MONTHS of the mailing date of this final action and the advisory action is not mailed until after

the end of the THREE-MONTH shortened statutory period, then the shortened statutory period

will expire on the date the advisory action is mailed, and any extension fee pursuant to 37

CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

however, will the statutory period for reply expire later than SIX MONTHS from the mailing

date of this final action.

25.   Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Chi-Chung E Lee whose telephone number is 703-306-4153.

The examiner can normally be reached on 8 am - 5 pm, Mon. - Fri..

        If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Gail O Hayes can be reached on 703-305-9711. The fax phone numbers for the

organization where this application or proceeding is assigned are 703-746-7239 for regular

communications and 703-746-7238 for After Final communications.

        Any inquiry of a general nature or relating to the status of this application or proceeding

should be directed to the receptionist whose telephone number is 703-305-3900.

Chi-Chung Lee
October 9, 2002

GAIL HAYES
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100